Abstract

A computer system analysis tool and method that will allow for qualitative and quantitative assessment of security attributes and vulnerabilities in systems including computer networks. The invention is based on generation of attack graphs wherein each node represents a possible attack state and each edge represents a change in state caused by a single action taken by an attacker or unwitting assistant. Edges are weighted using metrics such as attacker effort, likelihood of attack success, or time to succeed. Generation of an attack graph is accomplished by matching information about attack requirements (specified in "attack templates") to information about computer system configuration (contained in a configuration file that can be updated to reflect system changes occurring during the course of an attack) and assumed attacker capabilities (reflected in "attacker profiles"). High risk attack paths, which correspond to those considered suited to application of attack countermeasures given limited resources for applying countermeasures, are identified by finding "epsilon optimal paths."